Jurnal Manajemen Pendidikan *Volume 13, No. 02, 2025, halaman 379 - 382*
https://journal.unpak.ac.id/index.php/jmp *e-ISSN: 2614-3313 ; p-ISSN: 2302-0296*
Penerbit: Sekolah Pascasarjana, Universitas Pakuan

RISK MANAGEMENT IN THE OPERATION OF AUTOMATIC TELLER MACHINES CASE STUDY OF BANK SYARIAH INDONESIA MEDAN

Ali Mahadi Ritonga [a*)], Sugianto [a)], Ahmad Syakir [a)]

[a)] *Universitas Islam Negeri Sumatera Utara, Medan, Indonesia*

[*)]*e-mail korespondensi: alimahadiritonga@gmail.com*

Article history: received 01 June 2025; revised 12 June 2025; accepted 26 July 2025 ***DOI :*** https://doi.org/10.33751/jmp.v13i2.12626

Abstract. The purpose of this study is to analyze risk management in the operation of Automatic Teller Machine (ATM) at PT. Bank Syariah Indonesia. This study uses a descriptive qualitative method to test data through interviews. The results of this study show risk management in the management of Automatic Teller Machine (ATM). ATM operational risk management at BSI has been running with various security systems, but it still needs improvement, especially in terms of security risk mitigation, operational optimization, and customer education. With the strengthening of a more proactive strategy and the use of advanced technology, the effectiveness of ATM risk management at BSI can be further improved.

Keyword: risk management; automatic teller machine

I. INTRODUCTION

Islamic banking has rapidly developed in Indonesia, making it one of the options to help the country's economic growth. This is due to several advantages, one of which is the profit-sharing concept. The profit-sharing orientation is what enables Islamic banks to present themselves as an alternative or replacement for the interest system, which has long been questioned in terms of its legality by Muslims (Wahap, 2016). The development of technology will radically change the banking transaction system, which will ultimately transform the banking culture. Islamic banking is currently very much needed by society. From an Islamic perspective, Islamic banks are able to stand and compete with conventional banks and play an important role in the welfare of the community. This is in line with the basic principles of Islamic economics, which is a set of Islamic teachings that serve as a reference for all economic activities carried out by humans, based on the principles of monotheism, stewardship (organization), and welfare.Electronic banking usually uses electronic payment methods, such as ATMs, Debit Cards, Internet Banking, SMS Banking, Call Banking, IP Phone Banking, and other withdrawal cards (Dea Fathun, 2020). Similarly, Bank Syariah Indonesia Branch Medan strives to provide satisfactory services to its customers by offering sufficient facilities to attract their interest and ensure their loyalty to remain with Bank Syariah Indonesia. BSI in Medan is one of the branches of the largest Islamic banks in Indonesia. BSI provides various banking services in accordance with Islamic principles, such as savings, financing, investments, and other banking services. As part of the largest Islamic banking network in Indonesia, BSI has a significant responsibility in managing the operations of ATMs spread across various strategic locations. Banking services thru Automated Teller Machines (ATMs) have become a basic necessity for modern banking customers. ATMs provide convenience in conducting financial transactions such as cash withdrawals, inter-account transfers, bill payments, and balance inquiries without having to visit a bank branch.

One of the facilities provided by banks for customers is the ATM, which aims to make transactions easier for customers by using information technology. ATMs also help banks optimize their services because they have features that greatly assist customers in conducting transactions (Ratna, 2020). ATMs offer many conveniences and security for users, such as providing a PIN that only the user can know. However, if the user incorrectly enters the PIN three times, the ATM will be automatically blocked (M. Nur Ryanto, & Rahmawati, Y., 2018). As the use of ATMs increases, banking also faces various risks that can disrupt operations and customer trust. Bank Syariah Indonesia (BSI) Medan, as one of the largest sharia banks in Indonesia, has an extensive ATM network to serve its customers. However, with the vastness of this ATM network, BSI Medan also faces various challenges in managing ATM operational risks. Success in managing ATM operational risks is not only important for maintaining the smoothness of banking services but also for preserving customer trust and the bank's reputation. Although BSI Medan has implemented various advanced technologies to ensure the smooth operation of ATM services, various risks can still threaten daily operational activities. These risks include technological, operational, security, and reputational risks, each of which requires appropriate attention and management. Technological risks in ATM operations include hardware, software, and network infrastructure failures. ATM machines that experience hardware malfunctions or system disruptions can cause inconvenience for customers and reduce trust in bank services. In addition, increasingly sophisticated cyberattacks also pose a serious threat to the security of customer data and transactions. Operational risks in ATM operations include human errors, non-compliance with operational procedures, and negligence in machine maintenance (Fatimah, 2014). Errors in cash replenishment, mistakes in card management procedures, and negligence in monitoring and routine maintenance can cause significant service disruptions. For security risks in ATM operations, it includes physical threats such as machine vandalism, cash theft, and ATM card fraud. Physical attacks on ATMs not only financially harm the bank but also disrupt service to customers. Additionally, reputational risk is related to the public's perception of the bank's ability to provide safe and reliable ATM services. Any disruption or security incident involving ATMs can damage the reputation of BSI Medan and reduce customer trust. Based on the risks that have been explained, it can be concluded that the problems often faced in ATM operations include system failures, machine malfunctions, cyber attacks, human errors, and security risks such as theft or vandalism of ATM machines. In 2022, BSI discovered thousands of cyber threats. Based on data in the BSI report, they found more than a thousand cybercrime threats throughout 2022, but none were ransomware attacks. This can be seen in the table below.

Table1. Cyber Crime Threats Against BSI (2022)

No	Data name	Account
1	*Phishing/social engineering*	1.767
2	*Skimming* di Atm Prima	232
3	*Skimming* di Atm Bersama	64

Source: databoks (2024)

Based on the table above, BSI experienced its first cyber attack in 2022. BSI discovered 1,767 phishing and social engineering attempts against its customers. Phishing is a cybercrime that involves sending fake web addresses to customers that look like the original website. BSI also identified 232 skimming cases on the Prima ATM network and 64 cases on the Bersama ATM network. Skimming is the act of stealing ATM card data by installing a special device in the ATM card slot to digitally copy the customer's card data (Ahdiat, 2023). From the explanation above, there are still shortcomings in BSI's risk management in handling its operational activities to address cyber attack cases. In the research (Dea Fathun, 2020), it is explained that the operational risks that frequently occur and one of the problems complained about by customers are the loss of ATM cards, ATM machine malfunctions, failed transfers, and transactions at shared ATMs. Although money does not come out of the ATM, the balance is only reduced due to machine errors. On the other hand, (Wulansari, 2023) states that complaints still frequently occur due to the large number of swallowed ATM cards and poor ATM network, which causes ATM transactions to be slower. In this study (Firmandani & Malik, 2019) explain that there is still exposure to operational risks, such as the ATM skimming case at Bank X which caused customers to lose money. The ATM skimming case indicates that the Bank's risk management is not yet optimal.

Based on the above description, it shows that previous research still lacks analysis regarding related risk management and cyber security, which are becoming increasingly relevant with the rise in cyber attack cases at present. This research aims to analyze cyber risk management in ATM operations, including security policies, early threat detection, and incident response.

Operational Risk Management Risk management is the activity of controlling the possibility or potential loss arising from natural conditions or speculative behavior. More specifically, it can be defined as a series of procedures and methodologies used to identify, measure, monitor, and control risks arising from business activities. "Risk management according to Bank Indonesia is a series of procedures and methods used to identify, measure, monitor, and control risks arising from business activities." (Taswan, 2020).

Automatic Teller Machine (ATM) Automatic Teller Machine (ATM) is an electronic service system provided for customers using computers to perform several banking functions automatically, which are usually carried out by tellers. ATMs can replace the role of tellers in serving various types of banking transactions. The operation of ATMs generally requires devices such as plastic cards and personal identification numbers (PIN).

II. METHOD RESEARCH

This research is a type of field research, which means that the study is conducted in the field, or the research location, to investigate the objective phenomena occurring there. Therefore, the data collection process is carried out directly in the field based on the informants' explanations. This research was conducted at Bank Syariah Indonesia in Medan City, North Sumatra. This research is a qualitative descriptive study, the purpose of which is to provide a description of a phenomenon, an event that is currently taking place. Meanwhile, qualitative research is inherently descriptive in nature. The data sources were obtained thru interviews conducted with the Manager, Mr. Ahmad Azwar, and the Customer Service (CS), Mrs. Dhea Vita Lestari, at Bank Syariah Indonesia KCP Kesawan. In addition to interviews, data was collected thru document studies. Data obtained thru descriptive analysis of qualitative data (Melong, 2015) means reducing data, which involves summarizing, selecting what is important, focusing on the important, finding patterns and themes, and discarding the unnecessary. By using abstraction, data can be reduced. Abstraction is an effort to create a main summary, procedures, and statements that must be retained to be included in the research data. In other words, researchers consistently carry out this data reduction process throughout the study to create core notes from the data they obtain from data mining. Data Presentation: A collection of information organized in a way that allows for drawing conclusions is called data presentation. Conclusion and Verification: Conclusion or verification is the final stage in the data analysis process.

III. RESULT AND DISCUSSION

Research Results Factors that potentially pose risks to Bank BSI Medan's ATMs include electrical malfunctions, lack of communication, poor network quality during transactions, and cyber security. Signal networks, ATM machine malfunctions, and external crimes are the causes of these risks. This BSI ATM can experience risks such as bank robbery or cyber theft. From the interview conducted with Mrs. Mulyani from PT. Bank Syariah Indonesia, she stated that "Many users have complained about the issue of ATM cards being swallowed and the suboptimal network quality on the ATM machines, causing the transaction process to take longer." One of the BSI ATM customers shared her experience that her ATM card was swallowed when she was about to make a transfer. She also forgot to take her ATM card, and when she returned, the card was swallowed again by the BSI ATM machine. However, after contacting Customer Service (CS), the issue was promptly and efficiently handled by the bank. Mrs. Dhea Vita Lestari, as the BSI CS, said that "If you experience an ATM card being swallowed, customers are advised to contact Customer Service (CS)." However, if the card is swallowed by an ATM from another bank, the bank will advise that the card be blocked first and then the repair process be carried out. This process requires the customer to bring their passbook, ID card, and pay a card replacement fee of Rp 25,000. Once the identification is complete, PT. Bank BSI proceeds with the risk measurement process to determine the extent of the risk caused by the ATM. Now the bank knows that the risk caused by internal factors does not fall into the category of high risk. However, this does not mean that every activity caused by internal factors does not pose a danger; it is possible that activities caused by internal factors can pose a danger. When customers conduct transactions and their ATM cards are swallowed, there is an irresponsible third party that steals the card data by installing a small device in the slot where the ATM card is inserted. This tool allows the perpetrator to obtain data and duplicate the bank card using information obtained thru phishing attacks or skimming methods. Skimming itself is the act of digitally stealing ATM card data with a special device that records data from the card without the customer's knowledge. After the transaction is completed, the card cannot be ejected. Theft can occur because irresponsible parties use small devices to discover PINs and any data considered confidential. According to a customer who used the BSI ATM, he experienced issues with a failed cash deposit and the balance not being credited to his account. reported a complaint to customer service (CS). After checking and removing the ATM machine, they did not know how much money had been deposited. Finally, the bank offered assistance by reporting to the head office within 14 working days. After that, they made a statement letter and waited for the results from the head office. On the other hand, Mrs. Mega, a customer who uses the BSI ATM, said, "I once had trouble with the mudharabah ATM because I couldn't withdraw cash at other ATMs."Next, BSI will gather information about the target risks and incidents. Operational risk monitoring is conducted to ensure that operational risks are within acceptable limits. The bank monitors ATMs by checking the machines once a week and using an application. For ATMs, the information technology (IT) division, the accounting division (vendor), and the business operations management (BSOM) division are responsible for risk management. Each of these parties has a specific area of expertise and will act according to customer complaints. In order to prevent internal and external risks and provide comfort and security for customers, this monitoring process must be frequently conducted by the bank. After identifying and analyzing the risks they will face in the future, BSI Bank must carry out the final stage, known as risk control. This stage aims to help the bank avoid, prevent, and minimize risks. The BSOM operational department must ensure that each work unit has adequate capability and knowledge regarding the information provided, so that the data is accurate. This aims to ensure that management can monitor and control ATM operational risks in a timely manner. Additionally, in terms of cybersecurity, Data Encryption can be implemented: All data sent from the ATM to the bank server must be encrypted to prevent unauthorized third parties from accessing it. Protection Against Skimming: Installing skimming detection devices on card slots and physical devices to prevent illegal installation of skimming devices. Regular Security Updates: Always update ATM software to close security gaps.

IV.CONCLUSSION

The conclusion from the analysis of the implementation of cybersecurity risk management in the operation of Automatic Teller Machines (ATMs) shows that ATM cybersecurity is a crucial aspect in protecting financial infrastructure, customer data, and the bank's reputation. The main risks faced by ATMs include threats such as malware attacks, skimming, DDoS attacks, and insider threats. To mitigate these risks, a structured approach is required that includes threat identification, risk assessment, and the implementation of appropriate controls and mitigation actions. In addition, the importance of a responsive incident response plan and regular evaluations thru security audits also emphasizes that risk management implementation must be an ongoing process. Banks and financial institutions need to continuously innovate in technology and cybersecurity policies to maintain ATM security in an increasingly complex digital era. By implementing this strategy, cyber security risks in ATM operations can be managed effectively, thereby protecting customers and avoiding financial and reputational losses for the bank. Based on the discussion above, PT. Bank BSI has implemented risk management in ATM operations. However, in an effort to enhance the sense of security and comfort for customers, PT. Bank BSI needs to increase the number of staff, particularly in the IT and technician departments, to monitor ATM conditions more optimally. In addition, BSI should also conduct more regular maintenance on the machines to prevent any unwanted issues.

REFERENCES

Arif & Desmarina. (2020). Marketing Skill. Medan: FEBI UINSU Press.

Ahdiat, A. (2023, Mei 10). *BSI Temukan Ribuan Ancaman Siber Pada Tahun 2022, Data Nasabah Diklaim Aman*. Retrieved from Databoks: https://databoks.katadata.co.id/datapublish/2023/04/10/bsi-temukan-ribuan-ancaman-siber-pada-2022

Amarani, Fauziah, Sugianto Sugianto, and Muhammad Lathief Ilhamy. "The Effect of Self-Efficacy and Self-Concept on Increasing Optimism in Achieving Targets in Employees of Bank Syariah Indonesia (BSI) Case Study of BSI KCP Medan Aksara." *Jurnal Manajemen Bisnis* 11.2 (2024): 985-998.

Anggraini, Tuti, Yenni Samri J. Nasution, and Sugianto Sugianto. "Lembaga keuangan syariah dan dinamika sosial (editor: Muhammad Yafiz)." (2015).

Awalia, Annisa Preity, Marliyah Marliyah, and Muhammad Lathief Ilhamy. "Analysis of financial performance assessment using the economic value added (EVA) method (study at Bank Muamalat Indonesia 2019-2021)." *Indonesian Journal of Economics and Management* 3.3 (2023): 618-629.

Basuki, H. &. (2021). Analisis Risiko Keamanan Siber Pada ATM dengan Menggunakan Kerangka Kerja NIST. *Jurnal Sistem Informasi Indonesia, 13(3)*, 152-165.

Dea Fathun, U. (2020). Analisis Manajemen Risiko Pada Operasional Automatic Teller Machine (ATM) Studi Kasus Pada PT Bank Aceh Syariah. *Diss UIN AR-RANIRY* .

Fatimah, N. (2014). Evaluating Operational Risk Management Practices in Islamic Banks of Pakistan. *Journal of Islamic Business and Management, 4*(2), 101-123.

Firmandani, W., & Malik, M. (2019). Analisis Manajemen Resiko Teknologi Informasi Pada Kasus Skimming ATM Bank X. *Jurnal Manajemen & Bisnis, 10*(1), 107-120.

Latumaerissa, J. R. (2011). *Bank dan Lembaga Keuangan lain.* Jakarta: Salemba Empat.

Marliyah, Marliyah, M. Ridwan, and Ayu Kartika Sari. "The Effect of E-Service Quality on Satisfaction and Its Impact on Customer Loyalty of Mobile Banking Users (Case Study of Bank Syariah Mandiri KCP Belawan)." *Budapest International Research and Critics Institute (BIRCI-Journal): Humanities and Social Sciences* 4.2 (2021): 2717-2729.

Ratna, D. (2020). Kepuasan Nasabah Pada Fasilitas Automatic Teller Machine (ATM) PT. Bank Muamalat Kota Bengkulu. *Skripsi IAIN Bengkulu*.

Rukin. (2019). Metodologi Penelitian Kualitatif. Sulawesi Selatan: Yayasan Ahmar Cendekia Indonesia.

Rustam, Bambang Rianto. (2013). Manajemen Risiko Perbankan Syariah Di Indonesia. Jakarta: Salemba Empat.

Saepul Hamdi, Sep dan Bahruddin, B. (2014). Metode Penelitian Kuantitatif Aplikasi Dalam Pendidikan.Yogyakarta: Deepublish.

Samita Dewi, Ida Ayu Made. (2019). Manajemen Risiko. DenpasarBali: UNHI Press.

Saragih, Noprillia Ramadhani, Muhammad Lathief Ilhamy, and Muhammad Ikhsan Harahap. "The Effect of Person Organizational Fit (PO-Fit) and Organizational Commitment on Employee Performance through Organizational Citizenship Behavior (OCB) as Intervening Variable (Case Study Of Bank BSI KCP Stabat Proklamasi)." *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)* 6.3 (2023): 2186-2200.

Suharto, S. &. (2020). Analisis Risiko Keamanan Sistem Informasi Perbankan Menggunakan Kerangka Kerja ISO 27005. *Jurnal Teknologi dan Sistem Informasi, 14(2)*, 135-142.

Suwito, Firdha Aigha, Sugianto Sugianto, and Nurul Jannah. "Analisis Pangsa Pasar Dengan Metode BCG Matriks Pada Perusahaan Farmasi Di Bursa Efek Indonesia." *EKONOMIKA45: Jurnal Ilmiah Manajemen, Ekonomi Bisnis, Kewirausahaan* 10.2 (2023): 21-33.

Taswan. (2020). *Manajemen Perbankan Konsep, Teknik, Aplikasi.* Yogyakarta: UPP STIM YKPN.

Wulansari, S. (2023). Analisis Manajemen Risiko Pada Operasional Automatic Teller Machine (ATM) Pada PT Bank Syariah Indonesia (BSI) KC Bengkulu S. Parman 2. *Skripsi Universitas Islam Negeri Fatmawati Sukarno Bengkulu*.